MIT SICHERHEIT IN DIE CLOUD

Wie spätestens auf der SPS IPC Drives 2017 deutlich wurde, verschmelzen Fertigungstechnik (Operation Technology; OT) und Information Technology (IT) immer stärker. Die Produktionssysteme erhalten immer mehr Tore nach außen, vor allem zum Internet und in die Cloud. Wer cyber-physikalische Systeme, das Internet der Dinge und Cloud-Computing nutzen möchte, um die Wettbewerbsvorteile einer vernetzten Produktion auszuschöpfen, muss daher auch für den Schutz von Daten und Programmen vor Verlust und Missbrauch durch unbefugten Zugriff sorgen. **Von Ing. Peter Kemptner, x-technik**

Um mit ihren Digitalisierungs-Ambitionen datentechnisch nicht in unkontrollierbare Graubereiche zu geraten, müssen Unternehmen die Ansprechpartner und Kompetenzen dafür ebenso klar regeln wie in der kaufmännischen IT. Ebenso wie dort muss die Cyber Security auch im Produktionsbereich eine sehr hohe Priorität erhalten, denn mangelndes Bewusstsein über Sicherheitslücken betrachten Hacker als Einladung. „Die Schnittstelle zwischen dem LAN – und damit dem Internet – und der Maschine ist aktuell das größte IT-Sicherheitsrisiko. Sie bedarf eines neuen Sicherheitsdenkens im Unternehmen“, erklärte Andreas Schlechter, Geschäftsführer des deutschen Security-Systemhauses Telonic nach der Messe in Nürnberg.

_Angreifer und ihre Ziele

Der Nerd, der aus Spaß am Gelegenheitserfolg systematisch nach Schwachstellen im Internet sucht, ist nicht der Hauptgegner, obwohl auch er erheblichen Schaden anrichten kann. Erpresserische Hacker konzentrieren sich zwar meist

Bildquelle: © Gorodenkoff - fotolia.com

auf Daten aus ERP- und CRM-Systemen, können aber ebenso durch Lahmlegen der Produktion oder – schlimmer – durch Manipulieren der Produktionseinstellungen zum Erfolg kommen. Allerdings ist der Aufwand dafür hoch und somit die Angriffswahrscheinlichkeit eher gering. Nicht zu unterschätzen sind Racheakte gekündigter Mitarbeiter.

Der Großteil aller für die Automatisierung relevanten Angriffe erfolgt unauffällig und ohne offensichtliche Störungen des Betriebs. Hinter ihnen steckt die Konkurrenz, die sich durch Spionage oder Sabotage einen Vorteil zu verschaffen hofft. Das deutsche BSI (Bundesamt für Sicherheit in der Informationstechnik) ortet zudem eine steigende Anzahl von Angriffen durch Nachrichtendienste von Ländern, die heimischen Unternehmen Vorteile verschaffen möchten.

_Wie sicher sind Daten in der Cloud?

Sind Daten (und Programme) einmal in der Cloud, sind sie auch sehr sicher. Die Anbieter von IT-Infrastruktur und Software „as a Service" unternehmen enorme Anstrengungen, um Verfügbarkeit und Zugriffsschutz hoch zu halten. Schließlich stünde ihr gesamtes Geschäftsmodell auf dem Spiel. Einzig zu bedenken ist, dass bei Rechenzentren in den USA nach dem Antiterror-Gesetz „Patriot Act" der Staat Zugriff erlangen kann. Wer das nicht möchte, sollte einem in Europa gehosteten Angebot den Vorzug geben.

>>

Auch der Weg der Daten in die Cloud und wieder zurück kann über die verwendeten Queuing-Protokolle wie MQTT (Message Queue Telemetry Transport) oder AMQP (Advanced Message Queuing Protocol) sehr zuverlässig und auch verschlüsselt erfolgen. Die ersten bereits auf dem Markt befindlichen Cloud-Buskoppler führender Automatisierungshersteller nutzen alle sicherheitstechnischen Möglichkeiten dieser Technologien.

An der Schnittstelle zwischen OT und IT setzt sich gerade OPC UA als neuer Standard durch, nicht zuletzt, weil das herstellerunabhängige Protokoll sehr sichere eingebaute Verschlüsselungsalgorithmen enthält. Man (die Gestalter der Softwarelösungen) muss diese allerdings auch verwenden.

_User-Management ist essenziell

Als wesentlichste Voraussetzung für eine IT-sichere Produktion im industriellen Internet der Dinge müssen sich Anlagenbetreiber zunächst klar werden, dass ihre vernetzten Produktionsmittel dieselbe Sorgfalt benötigen wie ihre restliche IT. Das beginnt mit dem Betrieb einzelner Anlagen in eigenen, vom Rest getrennten Netzwerksegmenten, sogenannten demilitarisierten Zonen (DMZ). Firewalls nicht nur vom Unternehmen nach außen, sondern auch zwischen funktional getrennten internen Einheiten verhindern das Übergreifen von Problemen, die man sich an einer Stelle eingehandelt hat, auf andere Bereiche.

Die meisten Angreifer von außen versuchen zunächst, an Berechtigungsinformationen (Passwörter) zu kommen. Eine rollenbasierte Rechtevergabe mit individueller Authentizierung für jeden einzelnen Mitarbeiter an allen Maschinen und Computern reduziert das Risiko. Ein RFID-Chip für jeden Mitarbeiter verhindert Vergessen und erübrigt die leider noch oft geübte Praxis eines per Klebeetikett bekanntgegebenen „Abteilungspassworts". Ist die Berechtigung auf dem Chip codiert und nicht nur auf dem Server in einer Tabelle hinterlegt, beißt sich der Hacker die Zähne aus.

Zahnlos bleiben solche Maßnahmen ohne eine aufmerksame Wartung: Die Berechtigungen ehemaliger Mitarbeiter müssen bei Beendigung des Dienstverhältnisses auch tatschlich gelöscht werden. Dieser Bereich verdient nicht zuletzt auch im Lichte der Ende Mai 2018 in Kraft tretenden EU-Datenschutzgrundverordnung (DSGVO) 2016/679 besondere Beachtung.

Apropos Wartung: Ein Motiv, Produktionseinrichtungen datentechnisch mit der Außenwelt zu verbinden, ist die Fernwartung. In zukünftigen Systemen wird diese durch eine vorausblickende Wartung aufgrund von Statusmeldungen aus den Maschinen und Anlagen erfolgen, oft im Rahmen von Instandhaltungsverträgen direkt durch den Hersteller. Der hat es im Griff, das Equipment so zu programmieren, dass die Kontaktaufnahme ausschließlich

Auch **per USB-Stick eingeschleuste Schadsoftware** (z. B. mit dem Video für die Nachtschicht) ist eine wesentliche Bedrohung.

in ausgehender Richtung erfolgt und Updates von der abholenden Produktionseinrichtung automatisch auf Echtheit überprüft werden können.

_Zu ebener Erde und im ersten Stock: Hybride IT

Wie in anderen Unternehmensbereichen ist auch in der Digitalisierung der Produktion gute Praxis, nicht alle Daten ungefiltert zur Bearbeitung in die Cloud zu schicken, sondern nur die relevanten Ergebnisse einer lokalen Vorverarbeitung. Weil das oft „am Rande des Unternehmens" passiert, hat sich dafür der Begriff Edge Computing eingebürgert. Eine hybride IT-Infrastruktur mit verteilten Systemteilen direkt an der Maschine, in der Produktionshalle, in der Unternehmenszentrale und in der Cloud bietet nicht nur erhebliche Kostenvorteile durch die geringeren Datenmengen. Die Möglichkeit, heikle Daten im Haus zu behalten und Daten ohne Meta-Informationen (z. B. Zahlen ohne Einheiten) reisen zu lassen, macht diese Daten für unehrliche Finder wertlos und erhöht so die Sicherheit.

_Genormte Security

Ein wichtiger Schritt in Richtung Datensicherheit ist die Normenreihe IEC 62443 „IT-Sicherheit für industrielle Leitsysteme – Netz und Systemschutz". Sie ist eine umfassende Arbeitsgrundlage für Anlagenbetreiber und Systemhersteller. Zentrales Element ist die Verpflichtung zum „Kontrollieren der Nutzung", die uns zu den Anforderungen an die rollenbasierte Berechtigungsvergabe zurückbringt.

Übrigens: Die Automobilbranche steckt sehr viel Geld in die Hacker-Abwehr und wir können uns darauf verlassen, dass die bekannten Automatisierungsanbieter alles in industrietauglicher Ausführung verfügbar machen werden, was dabei an für den Maschinen- und Anlagenbau sinnvollen Neuentwicklungen herauskommt.

www.automation.at